

Towards a TCP Security Option

Steven M. Bellovin

`smb@cs.columbia.edu`

`http://www.cs.columbia.edu/~smb`

Columbia University

November 9, 2006

TCP-MD5 Has Problems

TCP-MD5 Has Problems

Why Not Use IPsec?

Why Not use TLS?

Requirements for a
New Security Option

Protecting the TCP
Header

Key Identifier

Automated Key
Management

- Cryptographically weak — should use HMAC or other real MAC
- No KeyID to aid in key change
- No key management
- A waiver was required to permit progressing BGP4 on the standards track
- We need something better

Why Not Use IPsec?

TCP-MD5 Has Problems

Why Not Use IPsec?

Why Not use TLS?

Requirements for a New Security Option
Protecting the TCP Header

Key Identifier

Automated Key Management

- IPsec is hard to use for most applications
- IPsec plays poorly with NATs
- BGP speakers are rarely using NATted addresses, but (today's) router architectures aren't geared towards terminating IPsec directed at the control plane

Why Not use TLS?

TCP-MD5 Has Problems

Why Not Use IPsec?

Why Not use TLS?

Requirements for a New Security Option Protecting the TCP Header

Key Identifier

Automated Key Management

- TLS doesn't protect the TCP header
- Easy to destroy TCP sessions by packet injection
- Integrated key management too heavyweight for some applications

Requirements for a New Security Option

- Must protect crucial parts of TCP header
- Use proper cryptography
- Contain a key identifier
- Support automated key management

TCP-MD5 Has Problems

Why Not Use IPsec?

Why Not use TLS?

Requirements for a New Security Option

Protecting the TCP Header

Key Identifier

Automated Key Management

Protecting the TCP Header

TCP-MD5 Has Problems
Why Not Use IPsec?
Why Not use TLS?
Requirements for a New Security Option
Protecting the TCP Header
Key Identifier
Automated Key Management

- Should (authorized) middle boxes be able to do ACK-spoofing?
- Should port numbers be protected?
- What about window size?
- Congestion-related flags?
- TCP options?

Key Identifier

TCP-MD5 Has Problems
Why Not Use IPsec?
Why Not use TLS?
Requirements for a New Security Option Protecting the TCP Header
Key Identifier
Automated Key Management

- Support intraconnection rekeying
- No particular format specified or implied
- Deliberately unspecified: is there a relationship between keys or KeyIDs for for multiple connections between the same pair of processes or users

Automated Key Management

TCP-MD5 Has Problems
Why Not Use IPsec?
Why Not use TLS?
Requirements for a New Security Option
Protecting the TCP Header
Key Identifier
Automated Key Management

- Need for automated key management described in RFC 4107
- Existing key management scheme may suffice
- Again, no implication on relationship of multiple connections